PATENT ABSTRACTS OF JAPAN

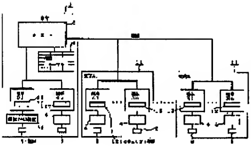
(11)Publication number : **09-134330**
(43)Date of publication of application : **20.05.1997**

(51)Int.Cl. G06F 15/00
G06F 1/00
G06F 12/14

(21)Application number : **07-289011**
(22)Date of filing : **07.11.1995**

(71)Applicant : **FUJITSU LTD**
(72)Inventor : **UCHIUMI KENJI**
YOSHIOKA MAKOTO
MURAKAMI KEIICHI

(54) SECURITY PROTECTION SYSTEM



(57)Abstract:
PROBLEM TO BE SOLVED: To realize the data security of a medium with an easy processing by reading intrinsic ID from the medium to be accessed and terminal ID from a terminal and permitting access to be possible to the medium only when they are correct.
SOLUTION: Intrinsic ID is read from the medium to be accessed by a security means 12 and terminal ID at every terminal is read from the terminal concerning the medium 5 where intrinsic ID is previously written and access is made to be possible only when intrinsic ID and terminal ID are correct. At this time, the security means 12 are provided at every terminal or every control program of the terminal and the ciphering and deciphering of medium data are executed by intrinsic ID and terminal ID. Besides, medium data is ciphered or deciphered by intrinsic ID, terminal ID and user ID. Therefore, when medium ID, intrinsic ID and terminal ID of the medium 5 are checked and recognized that they are OK, writing and reading ciphered data are made to be possible.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－134330

(43)公開日　平成９年(1997)５月20日

(51)Int.Cl.⁶	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　15/00	３３０		Ｇ０６Ｆ　15/00	３３０Ｃ
1/00	３７０		1/00	３７０Ｅ
12/14	３２０		12/14	３２０Ｆ

審査請求　未請求　請求項の数７　ＯＬ　（全　９　頁）

(21)出願番号　特願平7－289011

(22)出願日　平成７年(1995)11月７日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　内藤　研二
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　吉岡　誠
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　村上　敬一
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

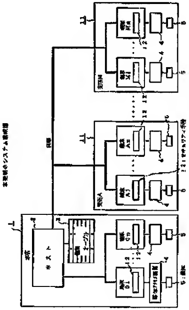
(74)代理人　弁理士　岡田　守弘

(54)【発明の名称】　セキュリティ保護システム

(57)【要約】

【課題】　本発明は、媒体上のデータのセキュリティを保護するセキュリティ保護システムに関し、媒体ＩＤ、固有ＩＤ、端末ＩＤをチェックしてＯＫとなったときに暗号化したデータの書き込み／読み出しを許可し．媒体のデータのセキュリティを簡単な処理で実現することを目的とする。

【解決手段】　固有ＩＤを予め書き込んだ媒体と．アクセスしようとする媒体からは固有ＩＤを、端末からは端末毎の端末ＩＤを読み出し．固有ＩＤが正しく．かつ端末ＩＤが正しいときにのみ媒体にアクセス可能とするセキュリティ手段を備えるように構成する。



【特許請求の範囲】

【請求項１】媒体上のデータのセキュリティを保護するセキュリティ保護システムにおいて、
固有ＩＤを予め書き込んだ媒体と、
アクセスしようとする上記媒体からは固有ＩＤを、端末からは端末毎の端末ＩＤを読み出し、固有ＩＤが正しく、かつ端末ＩＤが正しいときにのみ上記媒体にアクセス可能とするセキュリティ手段を備えたことを特徴とするセキュリティ保護システム。

【請求項２】上記セキュリティ手段は、各端末に備えたことを特徴とする請求項１記載のセキュリティ保護システム。

【請求項３】上記セキュリティ手段は、端末の制御プログラム毎に備えたことを特徴とする請求項１記載のセキュリティ保護システム。

【請求項４】上記固有ＩＤと端末ＩＤにより媒体データの暗号化あるいは復号化を行うことを特徴とする請求項１記載のセキュリティ保護システム。

【請求項５】上記固有ＩＤ、端末ＩＤ、および利用者ＩＤにより媒体データの暗号化あるいは復号化を行うことを特徴とする請求項１記載のセキュリティ保護システム。

【請求項６】上記固有ＩＤとして、媒体の媒体ＩＤ、およびシステム毎に固有な端末ＩＤとしたことを特徴とする請求項１記載のセキュリティ保護システム。

【請求項７】媒体から端末にプログラムをインストールする際に上記セキュリティ手段は、当該媒体に書き込まれている媒体ＩＤ、およびインストールしようとする端末の端末ＩＤが正しいときにのみ端末に制御プログラムをインストールすることを特徴とする請求項１記載のセキュリティ保護システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、媒体上のデータのセキュリティを保護するセキュリティ保護システムに関するものである。

【０００２】

【従来の技術】従来、ホストと回線を介して複数の端末が接続されたシステムにおいて、端末にインストールするプログラムや業務処理して結果をＭＯ（光磁気ディスク）などの多重にデータを書き込むことができる媒体に格納し、ホストから端末あるいは端末からホストに運搬することが行われている。この際、データを格納した媒体が紛失したときに他人に盗用されないように運搬を注意して行うようにしていた。

【０００３】また、媒体によってはパスワード（識別子）を書き込んでおき、読み出し時にそのパスワード（識別子）を入力しないと読み出せないようにし、媒体が万一紛失しても他人に盗用されないようにしていた。

【０００４】

【発明が解決しようとする課題】従来は、上述した前者の端末からホスト、ホストから端末へデータを格納した媒体を注意して運搬していたのでは、万一紛失した場合に他人に盗用されてしまう問題がある。

【０００５】また、後者のパスワード（識別子）を媒体に書き込んでおき、読み出した時にパスワード（識別子）を入力しないと読み出せないようにした場合には、パスワード（識別子）が盗用されたときはデータが他人に盗用されてしまう問題がある。

【０００６】本発明は、これらの問題を解決するため、媒体ＩＤ、固有ＩＤ、端末ＩＤをチェックしてＯＫとなったときに暗号化したデータの書き込み／読み出しを許可し、媒体のデータのセキュリティを簡単な処理で実現することを目的としている。

【０００７】

【課題を解決するための手段】図１を参照して課題を解決するための手段を説明する。図１において、アクセク装置４は、媒体５をアクセスするものである。

【０００８】セキュリティ手段１２は、端末に設け、セキュリティを管理するものである。次に、動作を説明する。固有ＩＤを予め書き込んだ媒体について、セキュリティ手段１２がアクセスしようとする媒体からは固有ＩＤを、端末からは端末毎の端末ＩＤを読み出し、固有ＩＤが正しく、かつ端末ＩＤが正しいときにのみ媒体にアクセス可能とするようにしている。

【０００９】この際、セキュリティ手段１２は、各端末に備えたり、あるいは端末の制御プログラム毎に備えたりするようにしている。また、固有ＩＤと端末ＩＤにより媒体データの暗号化あるいは復号化を行うようにしている。

【００１０】また、固有ＩＤ、端末ＩＤ、および利用者ＩＤにより媒体データの暗号化あるいは復号化を行うようにしている。また、固有ＩＤとして、媒体の媒体ＩＤ、およびシステム毎に固有な端末ＩＤとするようにしている。

【００１１】また、媒体から端末にプログラムをインストールする際にセキュリティ手段１２は、媒体に書き込まれている媒体ＩＤ、およびインストールしようとする端末の端末ＩＤが正しいときにのみ端末に制御プログラムをインストールするようにしている。

【００１２】従って、媒体５の媒体ＩＤ、固有ＩＤ、端末ＩＤをチェックしてＯＫとなったときに暗号化したデータを書き込んだり、読み出したり可能にすることにより、媒体の暗号化されたデータの読出／書込のセキュリティを簡単な処理で実現することが可能となる。

【００１３】

【発明の実施の形態】次に、図１から図８を用いて本発明の実施の形態および動作を順次詳細に説明する。

【００１４】図１は、本発明のシステム構成図を示す。図１において、本店１は、各種業務（例えば銀行業務）

を行うものであって、ここでは、ホスト２、権限テーブル３、および複数の端末などから構成されるものである。

【００１５】ホスト２は、本店１内の複数の端末、および回線やネットワークを介して接続された支店１１内の複数の端末を一括管理するものである。権限テーブル３は、管理者や利用者の権限を管理するものである（図３参照）。

【００１６】端末は、ホスト２と通信して業務処理（例えば銀行業務）を行ったり、媒体5にデータを書き込んだり読み出したりなどするものであって、ここでは、セキュリティ手段１２および媒体アクセス装置４を備えたものである。

【００１７】セキュリティ手段１２は、端末が扱うデータなどのセキュリティを管理するものであって、ここでは、媒体アクセス装置４によって媒体５にデータを暗号化して書き込む際のセキュリティなどを管理するものである（後述する）。

【００１８】媒体アクセス装置４は、媒体５にデータを読み書きする装置であって、例えばMO（光磁気ディスク装置）や、読み書き可能な光ディスク装置などである。媒体５は、媒体ＩＤ、システム固有の固有ＩＤ、端末ＩＤ、および暗号化されたデータなどを書き込んだり、読みだしたりする可搬媒体である。

【００１９】支店１１は、本店１のホスト２との間に回線やネットワークを介して接続されたものであって、複数の端末から構成されるものである。以下図１の構成の動作を順次詳細に説明する。

【００２０】図２は、本発明の媒体のオーソライズフローチャートを示す。図２において、Ｓ１は、一意の媒体ＩＤを書換不可能な領域に書き込む。これは、媒体５である例えばMO（光磁気ディスク）の所定領域にレーザビームで一意の媒体ＩＤを書換え不可能な形で書き込む（焼き切る）。これにより、媒体製造メーカが媒体５の出荷時に一意の媒体ＩＤを書換え不可能な形で書き込み、媒体５自身の偽造を防止する。

【００２１】Ｓ２は、管理者のパスワードの入力があるか判別する。これは、図１の本店１の端末の媒体アクセス装置４に、Ｓ１で媒体ＩＤを書き込んだ媒体４を挿入したときに、入力されたパスワードが権限テーブル３を参照して管理者のパスワードであるか判別する。ＹＥＳの場合には、入力されたパスワードが管理者のパスワードであって媒体５を初期化する権限があると判明したので、Ｓ３に進む。一方、ＮＯの場合には、入力されたパスワードが管理者のパスワードでなく、媒体５を初期化する権限が無いと判明したので、終了する。

【００２２】Ｓ３は、Ｓ２のＹＥＳで初期化する権限ありと判明したので、システム毎の固有ＩＤの決定を行う。これは、システム毎の固有ＩＤとして、例えばA銀行の企業固有ＩＤを決定する。

【００２３】Ｓ４は、媒体を初期化してオーソライズ媒体を作成する。これは、Ｓ３で決定した企業固有ＩＤをＳ１の媒体５に書き込む。以上によって、後述する図４に示すように、媒体５に、Ｓ１で当該媒体出荷時に媒体製造メーカで一意の媒体ＩＤが書換え不可の形で書き込まれ、次に、Ｓ４で企業固有ＩＤが書き込まれると共に必要に応じて他の領域（端末ＩＤ、暗号化されたデータを格納する領域など）の初期化を行い、当該企業の支店などで使用できる媒体（オーソライズ媒体という）を作成できたこととなる。

【００２４】図３は、本発明の権限テーブル例を示す。この権限テーブル３は、図示のようにユーザＩＤに対応づけて管理者あるいは一般ユーザなどの資格や権限、およびパスワードなどを登録するものである。この権限テーブル３にユーザＩＤが登録されており、かつ当該ユーザＩＤに対応づけて登録された資格や権限に対応して業務処理やデータを参照などの権限が決められている。この権限テーブル３を参照して入力されたユーザＩＤについて管理者の権限があり、かつそのパスワードが入力されたときに、既述した図２のＳ２のＹＥＳとなり、オーソライズ媒体（媒体ＩＤおよび企業固有ＩＤ（システム毎に固有な固有ＩＤ）を書き込んで初期化した媒体５）を作成できる。

【００２５】図４は、本発明のセキュリティ媒体情報例を示す。ここでは、媒体５に図示の下記のセキュリティ媒体情報を書き込む。

・媒体ＩＤ：出荷時に書き込む、媒体に一意な媒体ＩＤ

・企業固有ＩＤ：企業が本店で媒体初期化として行う（図２のＳ４）

・端末ＩＤ：読出／書込許可する端末の固有ＩＤ（媒体と端末とをロックする場合に必要であるが、制御プログラムを端末にロックする場合には不要）

・暗号化されたデータ

・その他

図５は、本発明の特定端末への媒体のロックフローチャートを示す（媒体と端末とをロックする場合に必要であるが、プログラムを端末にロックする場合には不要）。これは、既述した図２のフローチャートに従い、図１の本店１の管理者が媒体製造メーカから書換え不可の形で一意な媒体ＩＤをレーザなどでかき込まれた媒体５に、企業固有ＩＤを更に書き込むおよび初期化したオーソライズ媒体（図１のＳ４）について、Ｓ１１およびＳ１２で特定端末への媒体ロックを行うときのフローチャートである。

【００２６】図５において、Ｓ１１は、端末毎の一意な端末ＩＤを決定する。これは、図１の支店において、管理者が当該支店に設置された各端末に一意な端末ＩＤを決定する。例えば各端末が固有に持つ一意な装置ＩＤを端末ＩＤと決定する。

【００２７】Ｓ１２は、オーソライズ媒体に端末ＩＤを

５）が当該端末に一意にロックされたものと簡単な処理によって判別し、媒体５から暗号化されたデータを読み出して復号化し、保存することが可能となる。

【００４３】図８は、本発明の制御プログラムのインストールフローチャートを示す。これは、図１のセキュリティ手段のプログラム（制御プログラム）を媒体５から各端末にインストールし、当該端末でしか制御プログラムを起動できない（あるいは当該媒体５を端末にしか再インストールできない）ようにロックし、セキュリティ手段のプログラムが他の端末に無断でインストールされないように防止し、媒体５のデータの盗用を防止するためのものである。

【００４４】図８において、Ｓ４１は、プログラムの特定領域に管理者パスワードとシステム毎の固有ＩＤとを書き込む。Ｓ４２は、マスタープログラムをコピーして各支店へ配布する。

【００４５】Ｓ４３は、各支店の各端末にマスタープログラムをコピーする。Ｓ４４は、プログラムの別の特定領域に端末毎の一意な端末ＩＤを書き込む。これは、支店でマスタープログラムを端末にインストールしてその終わりの状態でマスタープログラムの特定領域に端末ＩＤを書き込んでマスタープログラムを特定端末に固定し、プログラム起動時にはプログラム内の端末ＩＤと、インストールした端末の端末ＩＤとが一致しないとマスタープログラムの起動を禁止するようにするためである（尚、媒体を端末にロックする場合には、マスタープログラムの特定領域に端末ＩＤを書き込んでマスタープログラムを特定端末に固定し、次回以降のインストール時には、媒体５上の端末ＩＤと、インストールする端末の端末ＩＤとが一致しないとマスタープログラムの再インストールを禁止するためである）。

【００４６】

【発明の効果】以上説明したように、本発明によれば、媒体５の媒体ＩＤ、固有ＩＤ、端末ＩＤをチェックしてＯＫとなったときに暗号化したデータを書き込んだり、読み出したりする構成を採用しているため、媒体の暗号化されたデータの読出／書込のセキュリティを簡単な処理で実現することができる。これらにより、媒体５上の一意な媒体ＩＤ、固有ＩＤ、端末ＩＤのチェックという簡単な処理によって制御プログラム（あるいは媒体５）が端末にロックされた正当なものの場合のみ媒体５のアクセス許可を認め、それ以外はアクセス禁止として媒体が万一他人に渡っても暗号化されたデータの読み出しを不可とし、次に処理に時間のかかるデータを暗号化して書き込んだり、読み出した暗号化されたデータを復号したりし、セキュリティの完全を期すことが可能となる。

【図面の簡単な説明】

【図１】本発明のシステム構成図である。

【図２】本発明の媒体のオーソライズフローチャートである。

【図３】本発明の権限テーブル例である。

【図４】本発明のセキュリティ媒体情報例である。

【図５】本発明の特定端末への媒体のロックフローチャートである。

【図６】本発明のデータの書込フローチャートである。

【図７】本発明のデータの読出フローチャートである。

【図８】本発明の制御プログラムのインストールフローチャートである。

【符号の説明】

１：本店
２：ホスト
３：権限テーブル
４：媒体アクセス装置
５：媒体
１１：支店
１２：セキュリティ手段

【図３】

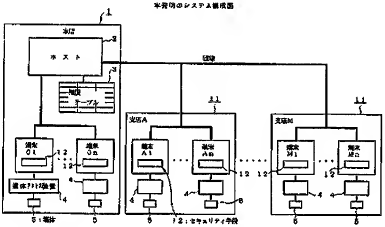
本発明の権限テーブル例

３

ユーザＩＤ	資格（権限）	パスワード	
×××	管理者／一般ユーザ	××××	

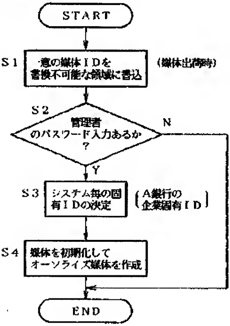
【図1】

本発明のシステム構成図



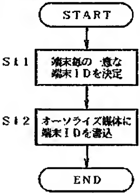
【図2】

本発明の媒体のオーソライズフローチャート



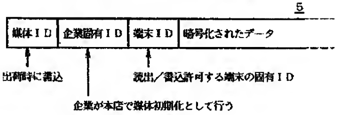
【図5】

本発明の特定端末への媒体のロックフローチャート



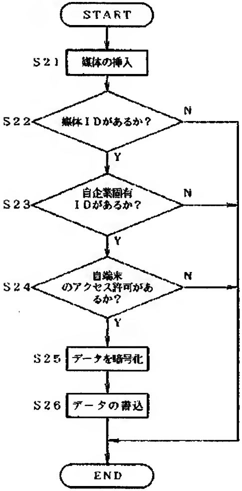
【図4】

本発明のセキュリティ媒体情報例



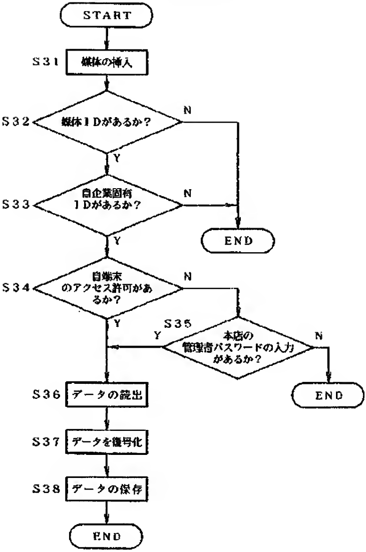
【図6】

本発明のデータ書込フローチャート



【図7】

本発明のデータの読出フローチャート



【図8】

本発明の制御プログラムのインストールフローチャート